

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-305558

(43)Date of publication of application : 22.11.1996

(51)Int.Cl. G06F 9/06  
 G06F 12/14  
 G09C 1/00  
 // H04L 9/00  
 H04L 9/10  
 H04L 9/12

(21)Application number : 07-104048

(71)Applicant : CASIO COMPUT CO LTD

(22)Date of filing : 27.04.1995

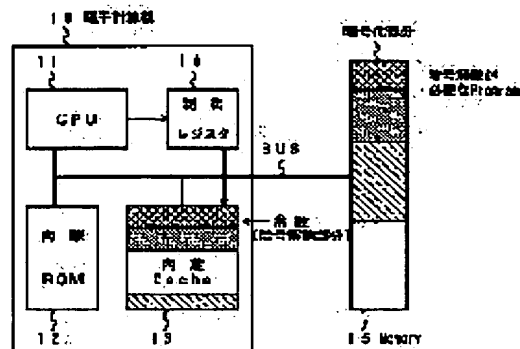
(72)Inventor : HIROYA TAKAYUKI

## (54) CIPHERING PROGRAM ARITHMETIC UNIT

## (57)Abstract:

PURPOSE: To prevent a ciphered program from being copied and in use in the ciphering program arithmetic unit mounted on an information terminal equipment or the like having a function decoding the ciphered program and executing it.

CONSTITUTION: An electronic computer 10 receives a ciphered part of a ciphered program loaded to an external memory 15, decodes the part according to a ciphering decoding program stored in advance in a built-in ROM 12 unable to be read to an external device and allows a built-in cache memory 13 to store the decoded program. Thus, an inhibit flag of a cache function is set to a control register 14 corresponding to a storage area of the decoded program stored in the built-in cache memory 13 to inhibit the decoded program from being read at an external bus and a CPU 11 executes a combination of the decoded program and the program being non-ciphered parts stored in the external memory 15.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-305558

(43) 公開日 平成8年(1996)11月22日

(51) Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0		G 0 6 F 9/06	5 5 0 A
	12/14			3 2 0 B
G 0 9 C 1/00	3 1 0	7259-5 J	G 0 9 C 1/00	3 1 0
// H 0 4 L 9/00			H 0 4 L 9/00	Z
9/10				

審査請求 未請求 請求項の数 4 O L (全 7 頁) 最終頁に続く

(21) 出願番号 特願平7-104048

(22) 出願日 平成7年(1995)4月27日

(71) 出願人 000001443

カシオ計算機株式会社

東京都新宿区西新宿2丁目6番1号

(72) 発明者 廣谷 孝幸

東京都羽村市栄町3丁目2番1号 カシオ  
計算機株式会社羽村技術センター内

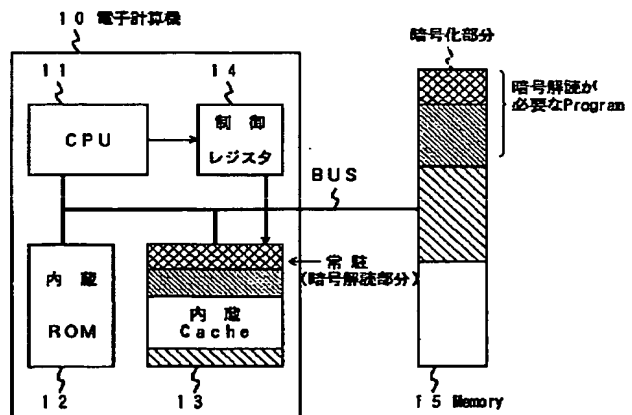
(74) 代理人 弁理士 鈴江 武彦

## (54) 【発明の名称】 暗号化プログラム演算装置

## (57) 【要約】

【目的】暗号化プログラムを解読して実行する機能を有する情報端末機器等に搭載される暗号化プログラム演算装置において、暗号プログラムがコピーされて利用されるのを防止すること。

【構成】外部メモリ15にロードされた暗号化プログラムの暗号部分を電子計算機10に取込んで、外部バスに読出し不可能な内蔵ROM12に予め記憶されている暗号解読プログラムに従って解読し、内蔵キャッシュメモリ13に記憶させると共に、この内蔵キャッシュメモリ13の前記解読されたプログラムの記憶領域に対応させて、制御レジスタ14にキャッシュ機能の禁止フラグをセットすることで該解読されたプログラムの外部バスへの読出しも禁止し、この解読後プログラムと前記外部メモリ15に記憶されている非暗号化部分のプログラムと組合されてCPU11により実行される。



**【特許請求の範囲】**

**【請求項 1】** 少なくとも暗号解読プログラムを記憶している第 1 のメモリと、

この第 1 のメモリに記憶された暗号解読プログラムにより解読された暗号プログラムを記憶する第 2 のメモリと、

この第 2 のメモリに記憶された解読された暗号プログラムの外部への読出しを禁止する読出し禁止手段とを具備したことを特徴とする暗号化プログラム演算装置。

**【請求項 2】** さらに、前記暗号プログラムの実行モードを記憶する制御レジスタを備え、

この制御レジスタの内容に従って前記第 2 のメモリに記憶された解読された暗号プログラムの外部への読出しを禁止することを特徴とする請求項 1 記載の暗号化プログラム演算装置。

**【請求項 3】** 前記暗号解読プログラムにより解読された暗号プログラムを第 2 のメモリに記憶させる際に、読出し禁止フラグを付けて外部への読出しを禁止することを特徴とする請求項 1 記載の暗号化プログラム演算装置。

**【請求項 4】** 前記第 2 のメモリはキャッシュメモリであり、暗号プログラムの実行時は、解読された暗号プログラムの記憶領域の追出し、書込みを禁止することを特徴とする請求項 2 又は請求項 3 何れか 1 項記載の暗号化プログラム演算装置。

**【発明の詳細な説明】****【0001】**

**【産業上の利用分野】** 本発明は、暗号化プログラムを解読して実行する機能を有する情報端末機器等に搭載される暗号化プログラム演算装置に関する。

**【0002】**

**【従来の技術】** 近年、コンピュータの急速な普及に伴って、そのソフトウェアも様々な種類のものが考えられ、汎用ソフトウェアとしてコンピュータの機種に関係なく利用できるようになっている。

**【0003】** その反面、ソフトウェアの違法なコピーも増加しており、早急にコピー防止の対策を施す必要がある。そこで、ソフトウェアのコピー防止対策の 1 つとして、ソフトウェアを暗号化し、その実行が許可されたユーザだけが解読プログラムを用いて暗号を解読して利用できるようにしたコピー防止方法が考えられている。

**【0004】** ここで、従来の暗号化手法は、ソフトウェアによる変換形態を利用したものが主なものであり、その変換アルゴリズムが複雑であればある程、解読が困難であるのは当然であるが、実際にその暗号化アルゴリズムを作成するのは非常に困難な作業である。

**【0005】**

**【発明が解決しようとする課題】** しかしながら、従来は、暗号解読用のプログラム自体がコピーされて解読されてしまったり、解読された後の暗号プログラムがコピ

ーされて利用される等の問題が生じていた。

**【0006】** 本発明は、前記のような問題に鑑みなされたもので、暗号プログラムがコピーされて利用されるのを防止することが可能になる暗号化プログラム演算装置を提供することを目的とする。

**【0007】**

**【課題を解決するための手段】** すなわち、本発明の請求項 1 に係わる暗号化プログラム演算装置は、少なくとも暗号解読プログラムを記憶している第 1 のメモリと、この第 1 のメモリに記憶された暗号解読プログラムにより解読された暗号プログラムを記憶する第 2 のメモリと、この第 2 のメモリに記憶された解読された暗号プログラムの外部への読出しを禁止する読出し禁止手段とを具備したことを特徴とする。

**【0008】** また、本発明の請求項 2 に係わる暗号化プログラム演算装置は、前記請求項 1 に係わる暗号化プログラム演算装置にあって、さらに、その暗号プログラムの実行モードを記憶する制御レジスタを備え、この制御レジスタの内容に従って前記第 2 のメモリに記憶された解読された暗号プログラムの外部への読出しを禁止することを特徴とする。

**【0009】** また、本発明の請求項 3 に係わる暗号化プログラム演算装置は、前記請求項 1 に係わる暗号化プログラム演算装置にあって、その暗号解読プログラムにより解読された暗号プログラムを第 2 のメモリに記憶させる際に、読出し禁止フラグを付けて外部への読出しを禁止することを特徴とする。

**【0010】** また、本発明の請求項 4 に係わる暗号化プログラム演算装置は、前記請求項 2 又は請求項 3 何れか 1 項に係わる暗号化プログラム演算装置にあって、その第 2 のメモリはキャッシュメモリであり、暗号プログラムの実行時は、解読された暗号プログラムの記憶領域の追出し、書込みを禁止することを特徴とする。

**【0011】**

**【作用】** つまり、前記請求項 1 に係わる暗号化プログラム演算装置では、第 1 のメモリに記憶された暗号解読プログラムにより解読された暗号プログラムが第 2 のメモリに記憶され、この第 2 のメモリに記憶された解読された暗号プログラムの外部への読出しが禁止されることになる。

**【0012】** また、前記請求項 2 に係わる暗号化プログラム演算装置では、請求項 1 に係わる暗号化プログラム演算装置にあって、暗号プログラムの実行モードを記憶する制御レジスタの内容に従って第 2 のメモリに記憶された解読された暗号プログラムの外部への読出しが禁止されることになる。

**【0013】** また、前記請求項 3 に係わる暗号化プログラム演算装置では、請求項 1 に係わる暗号化プログラム演算装置にあって、暗号解読プログラムにより解読された暗号プログラムが第 2 のメモリに記憶される際には、

読出し禁止フラグが付けられて外部への読出しが禁止されることになる。

【0014】また、前記請求項4に係わる暗号化プログラム演算装置は、請求項2又は請求項3何れか1項に係わる暗号化プログラム演算装置にあって、第2のメモリがキャッシュメモリとされ、暗号プログラムの実行時には、解読された暗号プログラムの記憶領域の追出し、書き込みが禁止されることになる。

【0015】

【実施例】以下図面により本発明の実施例について説明する。図1は本発明の第1実施例に係わる暗号化プログラム演算装置を搭載した電子計算機10の構成を示すブロック図である。

【0016】この電子計算機10は、CPU11を備えている。前記CPU11は、内蔵ROM12に予め記憶されているプログラムに従って回路各部の動作制御を実行するもので、このCPU11には、データ及び制御バスを介して前記内蔵ROM12の他、内蔵キャッシュメモリ13が接続される。

【0017】前記内蔵キャッシュメモリ13は、その記憶領域を選択的に指示する制御レジスタ14のセット“1”/リセット“0”によって、当該選択領域におけるキャッシュ機能（データの追出し、書き込み機能）の禁止/禁止解除が制御される構成とする。

【0018】また、前記CPU11は、外部メモリ15に記憶されているプログラムの読込みを行なった場合には、その読込んだプログラムに従って制御動作を実行する。ここで、前記内蔵ROM12には、予め暗号解読プログラムが記憶され、また、この内蔵ROM12の記憶内容は、外部バスには読出しできない構成とする。

【0019】なお、前記外部メモリ15に記憶されるプログラムデータは、例えば公共の有線放送や無線放送、あるいはメモリカード等の利用により得られるデータであってもよい。

【0020】そして、前記外部メモリ15から読込まれたプログラムデータが、暗号解読の不要な通常のプログラムデータである場合には、CPU11は内蔵キャッシュメモリ13の全ての領域についてキャッシュ機能を通常に使用してその読込みプログラムデータにそのまま従った制御動作を実行する。

【0021】次に、前記第1実施例の構成による暗号化プログラム演算装置を搭載した電子計算機10における暗号化プログラムの実行動作について説明する。図2は前記第1実施例に係わる暗号化プログラム演算装置を搭載した電子計算機10における暗号化プログラムの実行処理を示すフローチャートである。

【0022】すなわち、暗号解読が必要な暗号化プログラムが外部メモリ15にロードされると、この暗号化プログラムは電子計算機10に取込まれその暗号部分の解読が開始される（ステップS1、S2）。

【0023】前記暗号化プログラムは、そのプログラム全体の一部あるいは全てがコマンド、データの区別なく暗号化されており、ヘッダ等において暗号化プログラムであることが付加されているもので、電子計算機10は外部メモリ15から取込まれる暗号化プログラムをそのヘッダ等に付加された情報に基づいて暗号化プログラムであることを判断し、暗号部分の解読を開始する。

【0024】前記外部メモリ15から暗号化プログラムの暗号部分が電子計算機10から取込まれると、その暗号部分は、内蔵ROM12に予め記憶されている暗号解読プログラムに従って解読されるもので、この暗号解読プログラムに従って解読されたプログラムは、内蔵キャッシュメモリ13に書込まれる（ステップS3、S4）。

【0025】ここで、前記内蔵ROM12の記憶内容は、外部バスには読出しできない構成とされるので、暗号解読プログラムのアルゴリズムが第三者に解析される恐れはない。

【0026】そして、前記暗号化プログラムの暗号部分が解読され、内蔵キャッシュメモリ13に書込まれると、この解読されたプログラムの記憶領域におけるデータパージ等のキャッシュの機能を制御するための制御レジスタ14に対して、キャッシュ機能の禁止を指示するフラグをセットし、解読されたプログラムの外部バスへの読出し禁止が図られる（ステップS5）。

【0027】こうして、内蔵キャッシュメモリ13のキャッシュ機能の禁止領域において書込まれた解読されたプログラムは、前記外部メモリ15にロードされた暗号化プログラムの中のもともと暗号化されていない部分の非暗号部分のプログラムと組合され、CPU11に読出されて実行される（ステップS6、S7）。

【0028】つまり、前記外部メモリ15にロードされた暗号化プログラムのうち、その暗号部分のプログラムは、解読されて電子計算機10の内蔵キャッシュメモリ13の一部に常駐し、また、それ以外の非暗号部分のプログラムは、キャッシュメモリ13の残りの部分を用いて通常のキャッシュ動作によって実行される。

【0029】この後、前記暗号化プログラムの実行が不要になった場合には、内蔵キャッシュメモリ13に書込まれた暗号解読後のプログラムが消去されると共に、その記憶領域に対応させて、制御レジスタ14におけるキャッシュ機能禁止のフラグが解除される。

【0030】したがって、前記第1実施例の構成の暗号化プログラム演算装置を搭載した電子計算機10によれば、外部メモリ15にロードされた暗号化プログラムの暗号部分を電子計算機10に取込んで、外部バスに読出し不可能な内蔵ROM12に予め記憶されている暗号解読プログラムに従って解読し、内蔵キャッシュメモリ13に記憶させると共に、この内蔵キャッシュメモリ13の

前記解読されたプログラムの記憶領域に対応させて、制御レジスタ14にキャッシュ機能の禁止フラグをセットすることで該解読されたプログラムの外部バスへの読出しも禁止し、この解読後プログラムと前記外部メモリ15に記憶されている非暗号化部分のプログラムと組合されてCPU11により実行されるので、暗号解読用のプログラム自体がコピーされて解読されてしまったり、解読された後の暗号プログラムがコピーされて利用される等の問題を、電子計算機10の簡単な構成変更により解消することができる。

【0031】これにより、暗号化プログラムを特定の電子計算機にて専用の暗号解読プログラムにより解読して利用する場合に、第三者にその解読プログラムや解読後プログラムが読出されることのない信頼性の高い暗号化プログラム演算装置を提供できる。

【0032】なお、前記実施例では、解読されたプログラムを内蔵キャッシュメモリ13に書込んだ際に、その書込み領域におけるキャッシュの機能を制御レジスタ14により禁止して、外部バスへの読出し禁止を図っているが、例えば図3及び図4における第2実施例の暗号化プログラム演算装置で示すように、前記内蔵キャッシュメモリ13に対する解読されたプログラムの書込みと同時にその読出し禁止フラグを付加する命令をCPU21のシステムプログラムに持たせる構成とすれば、前記キャッシュ機能の禁止／禁止解除を行なう制御レジスタが不要になるので、解読されたプログラムの読出しがより困難な構成とすることができる。

【0033】図3は本発明の第2実施例に係わる暗号化プログラム演算装置を搭載した電子計算機20の構成を示すブロック図である。この電子計算機20は、CPU21を備えている。

【0034】前記CPU21は、内蔵ROM12に予め記憶されているプログラムに従って回路各部の動作制御を実行するもので、このCPU11には、データ及び制御バスを介して前記内蔵ROM12の他、内蔵キャッシュメモリ13が接続される。

【0035】前記内蔵キャッシュメモリ13は、データ書込みに伴うCPU21からの強制書込み命令により、当該データ書込み領域におけるキャッシュ機能（データの追出し、書込み機能）の禁止が制御される構成とする。

【0036】また、前記CPU21は、外部メモリ15に記憶されているプログラムの読込みを行なった場合には、その読込んだプログラムに従って制御動作を実行する。ここで、前記内蔵ROM12には、予め暗号解読プログラムが記憶され、また、この内蔵ROM12の記憶内容は、外部バスには読出しできない構成とする。

【0037】なお、前記外部メモリ15に記憶されるプログラムデータは、例えば公共の有線放送や無線放送、あるいはメモリカード等の利用により得られるデータで

あってもよい。

【0038】そして、前記外部メモリ15から読込まれたプログラムデータが、暗号解読の不要な通常のプログラムデータである場合には、CPU11は内蔵キャッシュメモリ13のキャッシュ機能を通常に使用してその読込みプログラムデータにそのまま従った制御動作を実行する。

【0039】次に、前記第2実施例の構成による暗号化プログラム演算装置を搭載した電子計算機20における暗号化プログラムの実行動作について説明する。図4は前記第2実施例に係わる暗号化プログラム演算装置を搭載した電子計算機20における暗号化プログラムの実行処理を示すフローチャートである。

【0040】すなわち、暗号解読が必要な暗号化プログラムが外部メモリ15にロードされると、この暗号化プログラムは電子計算機20に取込まれその暗号部分の解読が開始される（ステップA1、A2）。

【0041】前記暗号化プログラムは、そのプログラム全体の一部あるいは全てがコマンド、データの区別なく暗号化されており、ヘッダ等において暗号化プログラムであることの情報が付加されているもので、電子計算機20は外部メモリ15から取込まれる暗号化プログラムをそのヘッダ等に付加された情報に基づいて暗号化プログラムであることを判断し、暗号部分の解読を開始する。

【0042】前記外部メモリ15から暗号化プログラムの暗号部分が電子計算機20から取込まれると、その暗号部分は、内蔵ROM12に予め記憶されている暗号解読プログラムに従って解読されるもので、この暗号解読プログラムに従って解読されたプログラムは、内蔵キャッシュメモリ13に書込まれる（ステップA3、A4）。

【0043】この場合、前記解読されたプログラムの内蔵キャッシュメモリ13への書込み処理は、CPU21からの強制書込み命令により行なわれ、該キャッシュメモリ13におけるプログラム書込み領域には、その書込みと同時に読出し禁止フラグがセットされ、外部バスへの読出しが禁止される。

【0044】一方、前記内蔵ROM12の記憶内容は、外部バスには読出しできない構成とされるので、暗号解読プログラムのアルゴリズムが第三者に解析される恐れはない。

【0045】こうして、内蔵キャッシュメモリ13に読出し禁止フラグが付加されて書込まれた解読されたプログラムは、前記外部メモリ15にロードされた暗号化プログラムの中のもともと暗号化されていない部分の非暗号部分のプログラムと組合され、CPU11に読出されて実行される（ステップA5、A6）。

【0046】つまり、前記外部メモリ15にロードされた暗号化プログラムのうち、その暗号部分のプログラム

は、電子計算機20の内蔵キャッシュメモリ13に書込まれた暗号解読後のプログラムに従って実行され、また、それ以外の非暗号部分のプログラムは、そのまま読出されて実行される。

【0047】この後、前記暗号化プログラムの実行が不要になった場合には、内蔵キャッシュメモリ13にセットされている読出し禁止フラグが解除され、そこに書込まれている暗号解読後のプログラムが消去される。

【0048】したがって、前記第2実施例の構成の暗号化プログラム演算装置を搭載した電子計算機20によれば、外部メモリ15にロードされた暗号化プログラムの暗号部分を電子計算機20に取込んで、外部バスに読出し不可能な内蔵ROM12に予め記憶されている暗号解読プログラムに従って解読し、内蔵キャッシュメモリ13にCPU21からの強制書込み命令により書込むと共に、この内蔵キャッシュメモリ13に対する前記命令によりそのプログラム書込み領域に対応させて読出し禁止フラグをセットし、この解読後プログラムと前記外部メモリ15に記憶されている非暗号化部分のプログラムと組合されてCPU21により実行されるので、暗号解読用のプログラム自体がコピーされて解読されてしまったり、解読された後の暗号プログラムがコピーされて利用される等の問題を、電子計算機20の簡単な構成変更により解消することができる。

【0049】よって、前記第1実施例の暗号化プログラム演算装置と比較して、キャッシュ機能の禁止/禁止解除を行なう制御レジスタが不要になるので、解読されたプログラムの読出しがより困難な構成とすることができる。

【0050】

【発明の効果】以上のように、本発明の請求項1に係わる暗号化プログラム演算装置によれば、第1のメモリに記憶された暗号解読プログラムにより解読された暗号プログラムが第2のメモリに記憶され、この第2のメモリに記憶された解読された暗号プログラムの外部への読出しが禁止されるようになる。

【0051】また、本発明の請求項2に係わる暗号化プロ

グラム演算装置によれば、請求項1に係わる暗号化プログラム演算装置にあって、暗号プログラムの実行モードを記憶する制御レジスタの内容に従って第2のメモリに記憶された解読された暗号プログラムの外部への読出しが禁止されるようになる。

【0052】また、本発明の請求項3に係わる暗号化プログラム演算装置によれば、請求項1に係わる暗号化プログラム演算装置にあって、暗号解読プログラムにより解読された暗号プログラムが第2のメモリに記憶される際には、読出し禁止フラグが付けられて外部への読出しが禁止されるようになる。

【0053】また、本発明の請求項4に係わる暗号化プログラム演算装置によれば、請求項2又は請求項3何れか1項に係わる暗号化プログラム演算装置にあって、第2のメモリがキャッシュメモリとされ、暗号プログラムの実行時には、解読された暗号プログラムの記憶領域の追出し、書込みが禁止されるようになる。よって、暗号プログラムがコピーされて利用されるのを防止することが可能になる暗号化プログラム演算装置を提供できる。

【図面の簡単な説明】

【図1】本発明の第1実施例に係わる暗号化プログラム演算装置を搭載した電子計算機の構成を示すブロック図。

【図2】前記第1実施例に係わる暗号化プログラム演算装置を搭載した電子計算機における暗号化プログラムの実行処理を示すフローチャート。

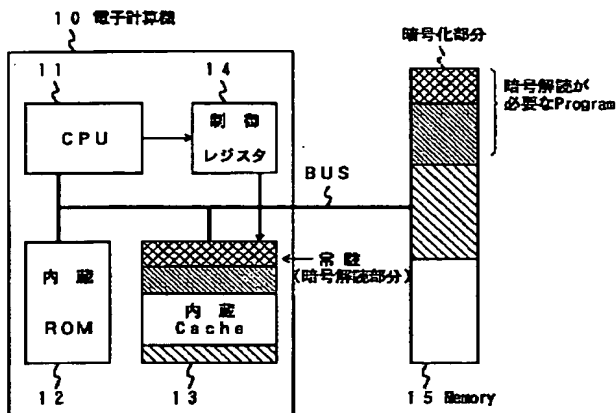
【図3】本発明の第2実施例に係わる暗号化プログラム演算装置を搭載した電子計算機の構成を示すブロック図。

【図4】前記第2実施例に係わる暗号化プログラム演算装置を搭載した電子計算機における暗号化プログラムの実行処理を示すフローチャート。

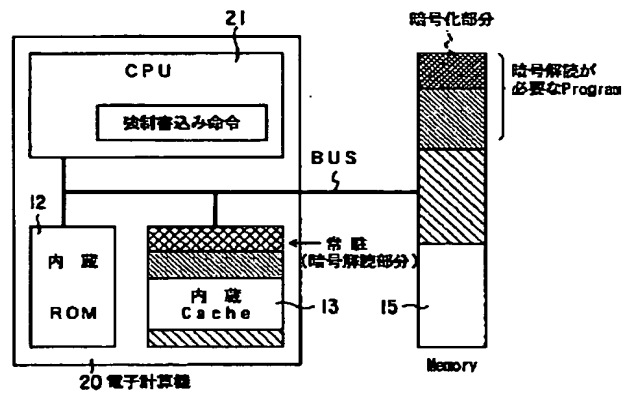
【符号の説明】

10、20…電子計算機、11、21…CPU、12…内蔵ROM、13…内蔵キャッシュメモリ、14…制御レジスタ、15…外部メモリ。

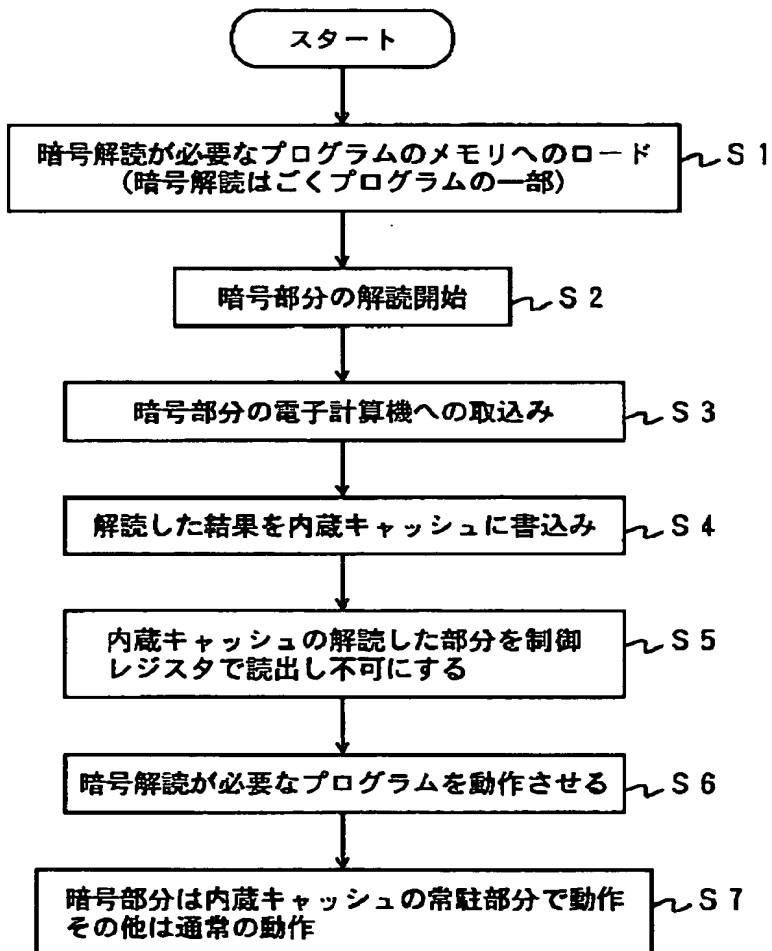
【図 1】



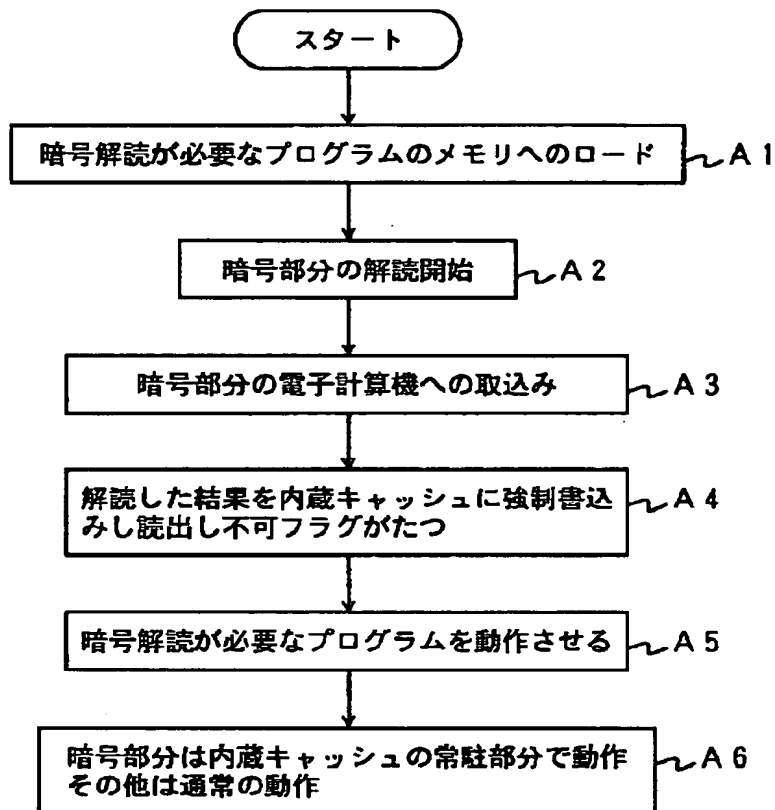
【図 3】



【図 2】



【図 4】



フロントページの続き

(51) Int. Cl.<sup>6</sup>

H 0 4 L 9/12

識別記号

庁内整理番号

F I

技術表示箇所